United Nations E/CN.15/2002/8

Economic and Social Council

Distr.: General
29 January 2002

Original: English

Commission on Crime Prevention and Criminal Justice
Eleventh session
Vienna, 16-25 April 2002
Item 5 of the provisional agenda*
International cooperation in combating transnational crime

Effective measures to prevent and control computer-related crime

Report of the Secretary-General

Contents

		Paragraphs	Page
I.	Introduction	1-3	2
II.	Status of ongoing efforts to prevent and control high-technology and computer-related crime	4-25	2
	A. General trends and developments	4-12	2
	B. Developments within the United Nations	13-22	4
	C. Developments in the work of other entities	23-25	7
III.	Concluding remarks	26	7

* E/CN.15/2002/1.

V.02-50946 (E) 040302 050302

I. Introduction

1. At its resumed tenth session, held on 6 and 7 September 2001, the Commission on Crime Prevention and Criminal Justice adopted a plan of action[1] dealing with the prevention and control of high-technology and computer-related crime as follow-up to and in implementation of paragraph 18 of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century, adopted by the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.[2]

2. In its resolution 56/121 of 19 December 2001, the General Assembly, expressing concern that technological advances had created new possibilities for criminal activity, in particular the criminal misuse of information technologies, recognizing the need to facilitate the transfer of information technologies, in particular to developing countries, underlining the need for enhanced cooperation among States in combating the criminal misuse of information technologies and stressing the role that could be played by the United Nations and other international and regional organizations, welcoming the work of the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders and recognizing with appreciation the work of the Commission on Crime Prevention and Criminal Justice at its ninth and tenth sessions, decided to defer consideration of the subject of the criminal misuse of information technologies pending work envisioned by the plan of action.

3. In its resolution 56/261 of 31 January 2002, the General Assembly took note of the plans of action with appreciation; called upon the Secretary-General to ensure the widest possible circulation of the plans; invited Governments to carefully consider them as guidance in the formulation of legislation policies and programmes; and invited the Secretary-General to consider carefully and implement, as appropriate, the plans, in accordance with medium-term plans and programme budgets and subject to available resources.

II. Status of ongoing efforts to prevent and control high-technology and computer-related crime

A. General trends and developments

4. The field of high-technology and computer-related crime continues to be characterized by rapid evolution on the part of offenders, preventive, legislative and law enforcement efforts and the underlying technologies themselves. During 2001, a number of States established or enhanced their capacities to deal with high-technology and computer-related crime as a specialized area of legislation and law enforcement. Legislative reforms included the creation of new offences, the expansion of existing offences and the modernization of investigative powers such as search and seizure and wiretapping authority to deal effectively with crime in the new electronic environments. That trend is expected to continue, in particular in Europe, where States are now engaged in implementing the Convention on Cybercrime, adopted by the Council of Europe in Budapest on 23 November 2001.[3]

5. The relationship between government crime control efforts and the role of the private sector companies involved in the production of hardware and software and in the delivery of services continued to be a major issue, at both the policy and legislative level and the investigative and law enforcement level in many countries. Major concerns included the extent to which crime control and investigative aids should be incorporated into new technologies, the costs of storing, intercepting and retrieving data sought by law enforcement agencies and a series of policy, criminal and civil liability issues arising from the relationships between the State, service providers and individual customers. Following a series of major virus and denial-of-service attacks during 1999 and 2000, a group of major high-technology companies established and funded a joint non-profit centre, the Information Technology Information Sharing and Analysis Centre, to set aside competitive rivalries and combine efforts against computer-related crime. Within major technology companies, the incorporation of security features into new software became a higher priority, as the companies sought to reduce their own vulnerability to attack and out of recognition that the fear of crime

and the presence of effective security features had become an important factor in the decisions of consumers shopping for new products.

6. The use of technical security and crime prevention methods continued to expand during 2001, a reflection of the nature of the technologies, their continuing expansion and the difficulties encountered by traditional legislative and law enforcement responses, in particular in transnational cases. These included established products such as programs to identify and screen out hostile programs such as worms and viruses from stored and transmitted data and barrier products such as firewall software. "Geolocation" programs, which identify the geographical source of online communications, were used increasingly to deny access to those located in jurisdictions where gambling, pornography or other activities are illegal. This was greeted positively by the law enforcement community, but criticized by advocates of a completely open Internet and experts who pointed out that the effective use of such programs depended on the willingness of web-site operators to use them and on their knowledge of the legal restrictions imposed by other countries. Most experts also agreed that such programs effectively prevented accidental breaches and were effective against unsophisticated offenders but not against more knowledgeable offenders, who could easily conceal their true geographical locations from the software and web-site operators using it. The use of filtering software, which identifies and blocks content inappropriate for children or other unauthorized users, also continued to expand and many operators of adult web sites incorporated products intended to trigger such software. Cryptographic applications were also used to protect sensitive communications and prevent users without permission from gaining access to proprietary or sensitive data.

7. Within the law enforcement community, investigators with the skills needed to intercept communications in high-speed, digital media, conduct successful searches of stored data, decrypt encrypted data and perform other similar functions were recognized increasingly as a scarce, valuable and specialized resource. Many agencies have now established specialized units, called upon to assist other investigators in areas ranging from counter-terrorism to drug trafficking and economic crime. Major concerns include the high costs and long-term investment represented by training investigators, the difficulty of retaining skilled investigators who can command higher salaries in better-funded private sector jobs and the simple problem of ensuring that investigators keep abreast of the deployment of new technologies and the latest criminal techniques for using them.

8. Member States are concerned about the potential offensive and defensive uses of new technologies by terrorist organizations and such concerns have been heightened considerably by the attacks of 11 September 2001. Experience shows that sophisticated terrorist offenders are already using the Internet to communicate. In that context, strong encryption and other security products have been used defensively to shield communications and stored data. The potential for offensive uses in support of terrorist objectives has also led a number of countries to establish specialized agencies dedicated to protecting data-processing, communication and other critical high-technology infrastructure from cyber-attacks.

9. The investigations that directly followed the September attacks also disclosed the use of the Internet to obtain information that could be used to plan attacks or obtain materials needed to make or improvise chemical, biological or radiological weapons. Several States that responded to a United Nations survey on, inter alia, the criminal misuse of explosives expressed their concern about the availability on the Internet of information about how to produce explosives and how to make explosive devices;[4] and a person arrested in connection with an attempt to detonate an explosive device concealed in his shoe while on board a commercial flight from Paris to Miami on 22 December 2001 was reported by media sources to have told investigators that he had made the device using information obtained from the Internet. Similar concerns were expressed on the part of agencies involved in drug law enforcement with respect to the availability of online information about how to produce synthetic drugs and where to obtain the necessary ingredients.

10. Other computer-related and high-technology offences also continued to raise concerns during 2001. Among the more prominent was the use of digital technologies and the Internet to produce and disseminate child pornography. Several participants in the Second World Congress against Commercial

Sexual Exploitation of Children, held in Yokohama, Japan, from 17 to 20 December 2001, linked possible increases in the exploitation of children and the overall volume of child pornography to that expanded market[5] but noted that a number of large-scale Internet child pornography operations, many of them transnational in scope, had been successfully broken up by cooperative law enforcement operations. Papers presented at the World Congress also linked the Internet to other paedophile activities, including child sex tourism and child abduction.

11. Concerns were also expressed about the increase in identity theft, in which personal data are used to allow offenders to impersonate the individual whose data were stolen. Combined with the anonymity of online transactions and other activities, identity thefts were used in connection with a range of crimes ranging from fraud to terrorist activities. Other criminal activities reported included an increasingly wide range of crimes involving fraud, online extortion, money-laundering and computer-assisted smuggling and crimes against computer systems and their users, involving viruses and other hostile programs and denial-of-service attacks. One new development with respect to fraud was the use of false Internet charities established to attract donations in the immediate aftermath of the terrorist attacks of 11 September, taking advantage of the fast reaction times possible with the establishment and removal of new web sites.

12. Online activities also created a number of emerging problems for national regulatory enforcement schemes in areas such as taxation, business regulation and the enforcement of environmental standards, where foreign storage of data, the increasing use of encryption and the ability of companies in one country to deal directly with customers in another have made regulatory, inspection and audit requirements more difficult to enforce. One example of this is the use of online pharmacies, which were identified as a problem in the report of the International Narcotics Control Board,[6] as well as by experts of the Customs Cooperation Council (also called the World Customs Organization) and by the Commission on Narcotic Drugs. The concern of the International Narcotics Control Board is primarily with the illicit shipment of narcotic drugs and psychotropic substances, but other sources suggest that the problem is broader, extending to many medicinal and other drugs that are subject to basic customs controls and medical prescription regimes in various countries. This poses a problem not only for criminal law enforcement, but also for health authorities, customs agencies and other regulatory bodies.

B. Developments within the United Nations

13. In its resolution 1999/23 of 28 July 1999, entitled "Work of the United Nations Crime Prevention and Criminal Justice Programme", the Economic and Social Council requested the Secretary-General, taking into account the activities of the workshop on crimes related to the computer network, held at the Tenth United Nations Congress on Crime Prevention and Criminal Justice, to conduct a study on effective measures that could be taken at the national and international levels to prevent and control computer-related crime. The report of the Secretary-General on the conclusions of the study was before the Commission at its tenth session (E/CN.15/2001/4). Several speakers acknowledged the gravity of high-technology and computer-related crime and emphasized the importance of taking action against such crime at the international level, including in the framework of the United Nations. It was noted that the fight against high-technology and computer-related crime required numerous sophisticated investigative measures and that following a common approach to fighting such crime was of vital importance.

14. The plans of action annexed to General Assembly resolution 56/261 for the implementation of and follow-up to the Vienna Declaration included a plan for action against high-technology and computer-related crime, which called upon the Centre for International Crime Prevention:

(a) To support national and international research activities to identify new forms of computer-related criminality and to assess the effects of such criminality in key areas such as sustainable development, protection of privacy and electronic commerce and the measures taken in response;

(b) To disseminate internationally agreed materials such as guidelines, legal and technical manuals, minimum standards, proven practices and model legislation to assist legislators and law enforcement and other authorities in the development,

adoption and application of effective measures against high-technology and computer-related crime and offenders both in general and in specific cases;

(c) To promote, support and implement, as appropriate, technical cooperation and assistance projects. Such projects would bring together experts in crime prevention, computer security, criminal legislation and procedures, prosecution, investigative techniques and related matters with States seeking information or assistance in those areas.

15. Pursuant to paragraph 5 of resolution 56/261, in which the General Assembly invited the Secretary-General to consider carefully and implement, as appropriate, the plans of action, including the plan of action against high-technology and computer-related crime, in accordance with the medium-term plans and the programme budgets and subject to available resources, and taking into account the comments made by the Commission at its tenth session,[7] a more detailed study of the problem and the actions set out in the plan of action will be undertaken as the necessary resources become available.

16. The increasing use of new computer and telecommunication technologies by organized criminal groups remains a matter of ongoing concern. This is particularly true for organizations that produce and traffic in narcotic drugs, which are among the most elaborate and best financed of criminal groups and therefore have access to the best available devices and expertise. The technologies are employed by producers and traffickers in much the same way as by legitimate commercial users. Information concerning the delivery of drug consignments is passed from sender to recipient using media that cannot easily be intercepted or read by law enforcement personnel. Business records are kept in foreign jurisdictions, concealed within large volumes of other data and protected by technologies such as firewalls and encryption to shield them from investigators. Electronic tracking of freight is used by traffickers to monitor items in which drugs or other contraband is concealed and, in the event of any undue delay, to alert them to possible discovery and interception of the shipment. The relative anonymity of electronic fund transfers is being used increasingly to pay for shipments without attracting the attention of law enforcement agents and by the recipients of the payments to launder them afterwards. The Internet is also being used to communicate basic information, such as instructions for the production of synthetic drugs and messages that encourage drug abuse.

17. In the report of the Secretariat of 21 December 2000 on the world situation with regard to illicit drug trafficking, the problem of electronic crime was considered and the recommendation made that Governments develop national policies supporting law enforcement responses (E/CN.7/2001/5, para. 150). Law enforcement agencies were called upon to liaise with service providers to ensure that relevant data was kept by the providers long enough to permit its recovery for investigative purposes and to work together in combating money-laundering via the Internet. In January 2002, a subsidiary body of the Commission, the Heads of National Drug Law Enforcement Agencies, Europe, held a regional meeting of experts to examine the problems faced by law enforcement agencies that encountered new technologies in drug-related investigations. The problems identified by the group included the enormous volumes of stored and transmitted data within which critical information must be identified and found; the increasing dependency of law enforcement on service providers to search for or intercept data and the cost- and security-related implications of this; and the advent of a range of new technologies, such as digital cellular telephones, satellite telephones and secure Internet chat rooms, which were harder to intercept than older methods of communication. Particular concerns were expressed about the advent of strong encryption products, which make intercepted or seized data difficult or impossible to read and which are becoming more common, both as applications that can be acquired and used by offenders and as integral "off-the-shelf" elements of electronic mail (e-mail), cellular telephone and other technologies.

18. In its reports for 1997,[8] 1998[9] and 2000,[10] the International Narcotics Control Board expressed concern about various ways in which new communication technologies were becoming a factor in illicit drug-related activities. In its report for 2001, the Board examined the problem in detail and made a series of recommendations. Generally, the Board noted that organized crime had become globalized and that the availability of new communication technologies had played a role in that development. In the case of international drug-related problems, the effects

included making the operations of producers, traffickers and other offenders more efficient and making the investigation and prosecution of such activities more difficult. The convergence of technologies had meant that offenders used not only computers and the Internet, but also facsimile machines, electronic pagers, pocket organizers and cellular telephones. Such devices are protected with encryption, firewalls and other security software and pre-paid accounts are used to avoid having to furnish service providers with true identities and geographical addresses for billing purposes. The Board also noted the occurrence of cases in which investigative targets had engaged in counter-offensive activities against law enforcement agencies. Some had hired professional security experts to assist in protecting their communications and data storage, while others had used "back-hacking" techniques to attack investigators' computers in an attempt to damage evidence or sabotage investigative efforts. In one case equipment had been stolen from investigators to gain the information needed to intercept their communications, with the result that the investigators were identified and threatened.[11]

19. While the use of new technologies to directly support drug trafficking was clearly a major concern, the Board also identified the use of Internet pharmacies as suppliers of prescribed narcotic drugs and psychotropic substances as a problem for national regulators and, more generally, noted the concerns of experts about the availability of information that encouraged illicit drug use or minimized the risks involved. The dissemination of information about how to produce illicit drugs and the availability of precursor chemicals and related information were also seen as problems.[12]

20. On a more positive note, the Board also examined the increasing use of secure Internet communications as the basis for international cooperation and noted that the Internet could also be used by international and national organizations as a means of prevention, by the dissemination of information to educate and dissuade potential drug abusers.[13]

21. The Board made a number of recommendations intended to ensure that drug enforcement personnel had adequate training, resources and legal powers to deal effectively with the problems mentioned. They related to the resources needed to attract skilled personnel, hardware and software needed to conduct investigations and sufficient critical infrastructure protection to shield investigations from sophisticated attacks. Several recommendations were directed at the positive use of technologies, in particular for education and prevention efforts, as well as cooperation between law enforcement, service providers and users of the technologies to identify and respond effectively to abuses. The Board also discussed the need for international cooperation and standards and recommended speedy ratification of the Council of Europe's Convention on Cybercrime, as well as consideration of the development of a United Nations convention against cybercrime.[14]

22. Following the World Congress held in Stockholm in August 1996, the Government of Japan hosted the Second World Congress against the Commercial Sexual Exploitation of Children in Yokohama from 17 to 20 December 2001, co-organized by the United Nations Children's Fund (UNICEF), End Child Prostitution in Asian Tourism (ECPAT) International and the NGO Group for the Convention on the Rights of the Child. UNICEF and a number of the non-governmental organizations and individual experts who attended expressed concern about the impact of new technologies on the sexual exploitation of children. A major focus of that concern was the ways in which the technologies supported, encouraged or facilitated the production and dissemination of child pornography. The advent of digital photography, for example, had made production much easier, while encryption and steganography were used to conceal pornography from investigators.[15] The Internet itself was used to disseminate child pornography, making relatively low-risk access easy, increasing demand and making detection, interdiction, investigation and seizure difficult. Ease of access and the reduction of risk to offenders were seen as factors contributing to increased demand for child pornography, leading to an increased risk for children. Other concerns were also expressed about new technologies. The use of the Internet by paedophiles to make anonymous contact with children, leading in some cases to abductions, was one such concern. In its concluding declaration, the Yokohama Global Commitment 2001, the Second World Congress called for the taking of adequate measures to address the negative aspects of new technologies, in particular the role played by the Internet in child pornography. It also recognized the potential for new technologies for